REMARKS/ARGUMENTS

Claims 1-16 are pending herein, claims 1 and 9 being independent. By this amendment, claims 1-13 and 15-16 are amended for cosmetic reasons and minor clarification to improve the form and readability thereof. In light of the remarks set forth below, Applicants respectfully submit that each of the pending claims is in condition for immediate allowance.

The Examiner has rejected claims 1-3, 5, 6, 9-11, 13 and 14 under 35 USC §103(a) as allegedly unpatentable over U.S. Patent No. 6,049,712 ("Wallinder") in view of U.S. Patent Publication 2003/0041245 ("Chan"); claims 8 and 16 under 35 USC §103(a) as allegedly obvious in light of Wallinder and Chan and further in view of U.S. Patent No. 6,289,223 ("Mukherjee"); claims 4 and 12 under 35 USC §103(a) as allegedly obvious in light of Wallinder and Chan in view of U.S. Patent Publication 2004/0132432 ("Moores"); and claims 7 and 15 as allegedly obvious under 35 USC §103(a) in view Wallinder and Chan and further in view of U.S. Patent No. 6,889,325 ("Sipman"). Applicants, having carefully considered the Examiner's rejections together with the comments provided in support thereof, respectfully request consideration and withdrawal of these rejections and submit that the invention as claimed is patentably distinct over the applied references, whether taken individually or in combination.

The following description is taken from the specification, and is provided for the convenience of the Examiner. It is not intended to argue limitations not present in the claims, or for any interpretation of claim terms that is narrower than would be understood by one of ordinary skill in the art in the context of the specification and claims as a whole.

The claimed invention is directed to a method and apparatus for authenticating a user of a terminal, e.g. a personal computer, that is connected to the Internet. See e.g., Paragraph 53 of the instant application. The authentication method relies on the security of a secure mobile network. See

Paragraph 20. The method of authenticating a user of a terminal generally comprises setting up a secure channel in a mobile network between an authentication unit that is connected to the Internet and a user's mobile equipment which is located in the vicinity of an Internet-connected terminal of the user. A digital code is downloaded to the terminal from the authentication unit via the Internet. A sound is generated by the terminal based on the received code. The nearby mobile equipment receives the generated sound through its microphone, and sends the received sound to the authentication unit via the secure channel of the mobile network.

Among the recitations of the independent claims not present in any of the cited references is establishment of a secure channel in a mobile network, and use of a mobile phone to send a received sound to the authentication unit, the sound being generated by the user terminal on the basis of a code sent to the terminal by the same authentication unit.

In Wallinder, a cell phone 2 comprises a memory for storing a PUI code and a PIN code. A fixed station 1 is connected to a local exchange LE 11. When the user wants access, the local exchange requests that the user provide the PUI and PIN codes. The user places the cellular phone close to the microphone of the fixed station 1 and the cellular phone emits prestored codes through its loudspeaker 4.

Unlike the recited subject matter of the pending claims, the terminal of Wallinder is connected not to the Internet, but to a local exchange or public switched telephone network (PSTN). Further, the code is not downloaded via the Internet to the terminal but is instead prestored in the mobile phone. As one skilled in the art will appreciate, the prestoring of codes on the mobile phone jeopardizes security as the codes can, for example, be recorded from the mobile phone and then used by unauthorized persons. Additionally, the sound is not generated by the terminal for authentication via the mobile phone. Thus, the sound is not received by the mobile phone but is

instead simply emitted by the mobile phone. Finally, the sound is not received by the SSCP 14 of Wallinder through a secure channel of a mobile network since the mobile switching center is not relevant in Wallinder. See Col. 5, lines 63-65.

Applicants also point out that although Figure 2 of Wallinder depicts a mobile network, Wallinder makes clear that radio connection is not a precondition for authentication. See Col. 8, lines 5-13. Figure 3 of Wallinder depicts an embodiment in which the codes are sent from an authentication center and stored at a service control point. However, the security of the mobile network is never used in the process of authenticating the fixed terminal.

In contrast, Applicants' claimed system and method of authenticating a terminal user recites establishment of a loop whereby the authentication unit interacts via the Internet with the terminal, which interacts with the mobile phone to transfer a sound, which then interacts via a secure channel of a mobile network, to thereby evaluate and confirm with the authentication unit a code. The secure channel established in the mobile network between the mobile phone and the authentication unit is used for authenticating the user terminal.

The addition of the teachings of Chan or of any of the other references fails to overcome the deficiencies of Wallinder as discussed above. Chan discloses a method of encoding a file and generating a digital signature using a private key, combining the encoded file with the signature and transmitting the same to the Internet. A digital signature is not a code as recited in Applicants' claims. Chan fails to disclose the alleged teaching for which it is cited.

Finally, Applicants submit that there is no teaching or suggestion for combining the teachings of Wallinder and Chan. The terminal 10a of Wallinder is not connected to the Internet and has no means for receiving a digital signature from the Internet as taught by Chan. Further, the mobile phone in Wallinder emits a code that is already stored in its memory and does not receive

any such code from the terminal. Thus, inasmuch as none of the prior art disclosures teach or suggest establishment of a secure channel in a mobile network that is used by a mobile phone to transmit a sound to an authentication unit, the sound being generated by a user terminal on the basis of a code sent via the Internet by the same authentication unit, all of Applicants' pending claims are deemed to be allowable over the cited references.

Applicants therefore request that the rejections be withdrawn.

Applicants have responded to all of the rejections recited in the Office Action. Reconsideration and a Notice of Allowance for all of the pending claims are therefore respectfully requested. If the Examiner believes that an interview would be of assistance, the Examiner is encouraged to contact the undersigned at the number listed below.

It is believed that no additional fees or charges are required at this time in connection with the present application. However, if any such fees or charges are required at this time, they may be charged to our Patent and Trademark Office Deposit Account No. 03-2412.

Respectfully submitted,
COHEN PONTANI LIEBERMAN & PAVANE LLP

By _____

Lance J. Lieberman
Reg. No. 28,437
551 Fifth Avenue, Suite 1210
New York, New York 10176
(212) 687-2770

Dated: July 16, 2008